Final Report for Period: 10/2010 - 12/2010
Submitted on: 01/03/2011
Principal Investigator: McLaughlin, Steven W.
Award ID: 0634952
Organization: GA Tech Res Corp - GIT
Submitted By:
McLaughlin, Steven - Principal Investigator
Title:
Physical Layer Security: Error Control Coding for Information Theoretic Security in Wireless and Beyond

Project Participants

Senior Personnel

Name: McLaughlin, Steven
Worked for more than 160 Hours: No
Contribution to Project:

Post-doc

Graduate Student

Name: Bloch, Matthieu
Worked for more than 160 Hours: No
Contribution to Project:
Matthieu Bloch spent the past summer in Portugal collaborating with Profs. Joao Barros and Miguel Rodrigues as part of the Luso-American Foundation matching to this project

Name: Klinc, Demijan
Worked for more than 160 Hours: Yes
Contribution to Project:
Demijan Klinc is working part-time on this project and will be spending some time in Porto later this year

Name: Harrison, Willie
Worked for more than 160 Hours: Yes
Contribution to Project:
Beginning graduate student

Name: Subramanium, Arun
Worked for more than 160 Hours: Yes
Contribution to Project:
Student is working as a graduate research assistant in the area of coding for physical layer security

Undergraduate Student

Technician, Programmer

Other Participant

Research Experience for Undergraduates

Organizational Partners

University of Porto

This project is being supported by a supplement from the Luso-American Foundation. We have had several long terms visits to/from Georgia Tech and the University of Porto in both directions related to this project. Those visits have resulted in several key publications that have just been submitted.

Other Collaborators or Contacts

Yes, as per the matching request with the Luso-American Foundation we are heavily engaged in a collaboration with the University of Porto. One of our students (Matthieu Bloch) spent the summer there and one Porto student (Joao Vielela) was in Atlanta for Fall 2007. Another GT student, Demijan Klinc has visited Porto in Spring 2009 and will be returning for Spring 2010

The collaboration has been very successful to date. We have several conference papers, two journal papers in preparation and one joint patent filed. Georgia Tech and Whisper Communications (a company founded by the PI) have agreed on an exclusive license for technology developed under the collaboration with the University of Porto.

Activities and Findings

Research and Education Activities:

We have been starting simulations in the area of wiretap security particularly and their application to the problem of 'information theoretic bit commitment.' This is a largely theoretical concept that has been developed over the years but has not seen wide practical application. Now we have developed some (albeit complex) algorithms to address this problem.

The first major paper on this award has just been published in a special issue of the IEEE Transactions on Information Theory (June 2008). The relevant conference in this area now has more than six sessions on this topic. Information- theoretic ideas are making their way into the main stream research community. The most recent IEEE Symposium on Information Theory (2009, Seoul) has six sessions on information-theoretic security - all of which have come out of two papers that were generated by our group. This is very exciting for us.

Our research activities have increased substantially in the last year (June 2008-June 2009). We have gone into two major areas and have some very nice results (described in the findings section). In addition to the research papers, we have filed three invention disclosures and are working towards licensing some of the technology as it relates to secure wireless communications. More specifically we have received some very early stage seed funding from the Georgia Research Alliance ($15,000) to validate several of our ideas in an RFID and 60 GHz wireless testbed. We hope to establish a very small company and seek SBIR funding in the next six months if our validation efforts work out as we have planned.

The research continues to bear a great deal of fruit in the year 2010. We have submitted four new journal papers related to the work, two of which we view as seminal work in the area. The SBIR proposal submitted to NSF mentioned above was funded and a spinout company Whisper Communications has made a great deal of progress in the last 6 months. Much of the technology being developed by Whisper was supported under this current grant. GT and Whisper are in the final stages of settling on an exclusive license agreement

for the technology.

In the final two months of the project the license agreement has been settled and Whisper Communications is off on a very good footing. We have recently secured additional commercialization funding from the State of Georgia to continue the work. We are in the midst of preparing a Phase 2 SBIR proposal to NSF after a very successful SBOR Phase 1.

In the last two months we have also made significant progress in defining and proving the first known coding scheme that provides strong security on the wiretap channel. A journal paper has recently been approved on that topic.

Findings:

Finding 1: Practical, classical, information-theoretic bit commitment is possible and that in some cases the protocol we have developed our approaches the fundamental limits of practical bit commitment.

Finding 2: The wireless protocols we have developed are practical and of interest to many in the information theory and cryptography communities. This protocol in some cases comes very close to the secrecy capacity limits predicted by theory. Our new codes under development could have considerable impact and we have been contacted by numerous companies who are interested in validating the concepts.

Finding 3: Information theoretic security concepts can be applied to areas such as cooperative communications, network attached storage and disc forensics.

Finding 4: We developed a new class of error correction codes for the Gaussian wiretap channels that are currently being validated in a wireless test bed. These error correction codes are based on low density parity check codes and have the property that they have good error correction abilities for the intended parties in communications and nearly no error correcting capability for the eavesdropping party. This is a remarkable property that allows any eavesdropper (for example in the next room who has a lower SNR) unable to decode and, in fact, have a bit error rate of 0.5 which translates to precisely zero information transfer.

Finding 5: We have started to show the impact that a physical-layer communication system has on the higher layers of the communications stack. More specifically, using the codes developed in Finding 4, we can show that the additional channel errors that are observed at the crypto layer have a profound effect on the security of the crypto layer. That is if we can assure that the eavesdropper has a bit error rate, of for example 0.1, then the eavesdroppers attacking ability increases by several order of magnitude. This allows us to use a lighter cryptographic protocol and maintain the same level of security.

Finding 6: We have shown that some standard tools in many communication systems, if used properly can be used to enhance the security of a system. For example data scrambling is a common tool used in communication systems to ensure a data spectrum that is white. We have shown that a scrambler in the evolving 60 GHz system and standard can be modified slightly to provide the kind of physical layer security described in previous finding.

Finding 7: a new class of codes that address the issue of 'strong secrecy' have been developed and a journal paper has been submitted. Strong secrecy is critical to the success of a physical layer security protocol. This higher level of secrecy is one that traditional security (e.g. cryptography) community believes in, and as we build bridges between these communities, is critical to wider adoption of physical layer principles.

Finding 8: the issue of defining an acceptable security criterion that meets the security

needs of the traditional community and maps well to the metrics common in the physical layer communications community continues to be one of the main challenges.

Finding 9: we have for the first time proposed and proved a new coding scheme which provides *strong* security on the wiretap channel. This is a coding scheme which asymptotically provide zero information to the wiretapper. This is in dramatic contrast to all of the other existing work which focuses on information theoretic (or weak) security which defines average, per letter security. This is a major advance in this area.

Training and Development:

Outreach Activities:
In July 2008 we gave a tutorial on 'Physical Layer Security' at the IEEE Symposium on Information Theory and had more than 100 attendees.

Journal Publications

M. Bloch, J. Barros, M. Rodrigues, S. McLaughlin, "Wireless Information Theoretic Security", IEEE Transactions on Information Theory, p. 2515, vol. 54, (2008). Published,

M. Bloch, R. Narasimha and S. W. McLaughlin, "Network Security for Client-Server Architecture using Wiretap Codes", IEEE Transactions on Forensic and Information Security, p. , vol. , (2008). Accepted,

J. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly Jamming for Wireless Secrecy", IEEE Transactions on Information Theory, p. , vol. , (2010). Accepted,

D. Klinc, J. Ha, J. Barros, and S. W. McLaughlin, "LDPC Codes for the Gaussian Wiretap Channel", IEEE Transactions on Information Forensics and Security, p. , vol. , (2010). Submitted,

A. Subramaniam, M. Bloch, A. Thangaraj, S. McLaughlin, "Strong Secrecy on the Binary Erasure Wiretap Channel Using Large-Girth LDPC Codes", IEEE Transactions on Information Forensics and Security, p. , vol. , (2010). Accepted,

W. Harrison, J. Almeida, J. Barros, and S. W. McLaughlin, "Coding and Cryptography: Physical-Layer Security through Stopping Sets", IEEE Transactions on Information Forensics and Security, p. , vol. , (2010). Submitted,

Books or Other One-time Publications

W. Harrison and S. McLaughlin, "Tandem coding and crypto on wiretap channels: EXIT chart analysis

", (2009). Conference publication, Published
Bibliography: IEEE International Symposium on Information Theory, Seoul, July 2009.

B.-J. Kwak, N.-O. Song, B.-S. Park, D. Klinc, D. S. Kwon, and S. W. McLaughlin, "Physical Layer Security with Yarg Code,", (2009). conference publication, Published
Bibliography: Conference on Information Sciences and Systems, Princeton, March 2009.

W. Harrison and S. McLaughlin, "Physical-Layer Security: Combining Error Control Coding and Cryptography", (2009). Conference publication, Published
Bibliography: IEEE International Conference of Communications, Communications Theory Workshop, June 2009.

A. Suresh, A. Subramanian, A. Thangaraj, M. Bloch and S. McLaughlin, "Coding for Strong and Weak Security in Wiretap Channel", (2010). Conference publication, Accepted
Bibliography: 2010 International Turbo Coding Symposium

W. Harrison, J. Almeida, D. Klinc , S. W. McLaughlin, and Joao Barros, "Stopping Sets for Physical-Layer Security", (2010). Book, Published
Bibliography: IEEE Information Theory Workshop, Dublin, Ireland. August 2010

Web/Internet Site

URL(s):
http://www.prism.gatech.edu/~gtg578i/
Description:

Other Specific Products

Contributions

Contributions within Discipline:
Our work is increasingly showing how information theoretic concepts can be integrated in the classical security and cryptographic community. We believe some of our contributions are slowly having that effect on both the theoretical and practical community. This is evidenced in the increasing number of sessions at two major conferences and now an entire conference dedicated to information theoretic security. There is also an new and entirely dedicated to information theoretic security conference dedicated to the topic (Oct 2008). We have been contacted by at least six companies who are trying to validate the concepts in prototypes.

Contributions to Other Disciplines:
For the first time researchers in the cryptographic community seem to be embracing some of the concepts, as evidenced by the joint conference on information theoretic security in Calgary in 2008 and again in 2009.

Contributions to Human Resource Development:

Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:

Conference Proceedings

Categories for which nothing is reported:

Activities and Findings: Any Training and Development

Any Product

Contributions: To Any Human Resource Development

Contributions: To Any Resources for Research and Education

Contributions: To Any Beyond Science and Engineering

Any Conference